広域分散環境におけるネットワーク利用技術の開発

服部裕之

インターネットには、セキュリティや、リソース間の協調手法等、課題が山積しているが、本研究は、これらに対する技術的な解を導き出すことを目標としている。

1997年度は広域ネットワークにおける認証実用化の問題に関する課題について開発・研究を行なった。

1．はじめに

オンラインショッピングなど、インターネット上で提供されるサービスが多様化するにつれて、インターネットにおける認証技術の確立は急務である。

現在、認証技術の主流となっているのは、暗号技術、それも公開鍵暗号方式である。公開鍵暗号方式は、メッセージの暗号化に使う鍵と復号化に使う鍵を互いに異なるものにできる。この性質を利用し、一方の鍵を公開（公開鍵）し、もう一方の鍵を秘密（秘密鍵）にすることができる。

公開鍵暗号方式を用いた暗号通信を行なう際、相手の公開鍵は、ネットワークを利用して入手するのが一般的である。ところが、ネットワーク上の通信には、なりますし、改竄など、セキュリティ的な問題がある為に、通信相手の公開鍵が正真正銘本人のものであるかどうかを、受信側で証明できるか否かは、重要な問題である。

この問題に対する解決策の一つは、第三者機関によって、ある者の公開鍵が偽造されたもので無いことを証明するという仕組みを用意することである。これは、ある者の公開鍵を、第三者機関のもつ秘密鍵で暗号化し、それをその者の「証明書」として発行することによって実現できる。

インターネットでは、この第三者機関のことを証明書発行局（CA—Certification Authority—）と呼んでいる。

本研究は、インターネットにおけるCAの運用に関する諸問題の考察と、証明書の応用分野の模索に主眼をおいている。

本年度は以下の項目について研究開発を行なった。なお、これらの多くは、ICAT（認証実用化実験協議会—Initiatives for Computer Authentification Technology—）との共同開発・研究として行った。

1．証明書検索機能の実現。

2．証明書を活用した認証サービスの実験。

2．証明書の検索

証明書を用いたアプリケーションで常に問題となるのは、通信する相手の証明書（公開鍵）をどのような手段を用いて入手するか、ということである。

たとえば、公開鍵暗号を応用した暗号方式（たとえば、S/MIMEやPGPなど）を用いて、暗号メイルを送信するモデルを考えてみる。この際、メイルの送信者はDEK（Data Encryption Key）などの交換の為に、送信相手の公開鍵を事前に入手する必要がある。

入手方法は、(1)直接、通信相手に尋ねる　(2)オンラインで検索できるシステムを構築する、などが考えられるが、迅速性を考慮すると、明らかに(2)に利がある。

2.1　証明書検索機能の実現

証明書の検索機能は、我々がICATにて開発した証明書発行局パッケージICAPに、証明書検索機能を追加することによって実現した。これは、証明書のシリアル番号や氏名、電子メールアドレスなどの検索キーを元に、該当する証明書データを返信、または、証明書の内容表示を行うという機能である。

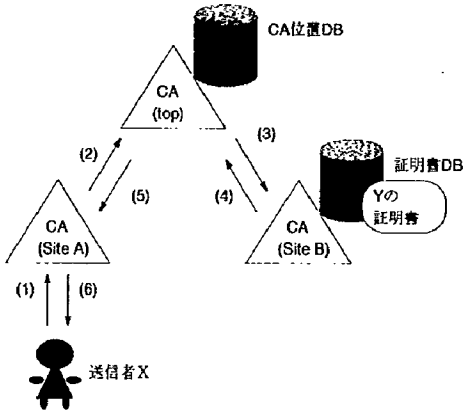
但し、当初、検索対象となる証明書は、あくまでもそのCAが自ら発行した証明書のみであり、他のCAが発行した証明書の検索は、後述のCA間の連携を考慮する必要があった。

ICAPの詳細については、文献(1)をご覧いただきたい。

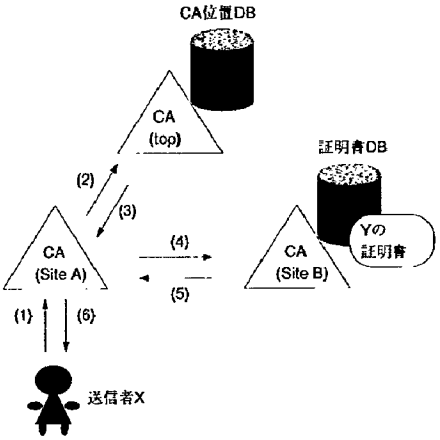
2.2　CA間連携モデル

次に、証明書の発行を複数のCAで分散して行っている場合の、証明書検索モデルを考察する。

CA間の連携のモデルとして、次の2つが考えられる。



●モデル 1



●モデル 2

モデル 1 において(1)(2)(3)のデータとは、通信相手の証明書の検索要求であり、(4)(5)(6)は、検索結果、つまり証明書のデータである。

一方、モデル 2 において(1)(2)のデータとは、通信相手の証明書の検索要求である。しかし上位 CA の返す値(3)は、モデル 1 とは異なり、相手の証明書データを保持している CA のアドレス（位置情報）である。このアドレスを元に、(4)で Site A は、Site B にもう一度証明書検索要求を行う。(5)(6)は、証明書のデータである。

CA 間連携モデルの詳細について、文献[2]をご覧いただきたい。

2.3 CA 間連携プロトコル

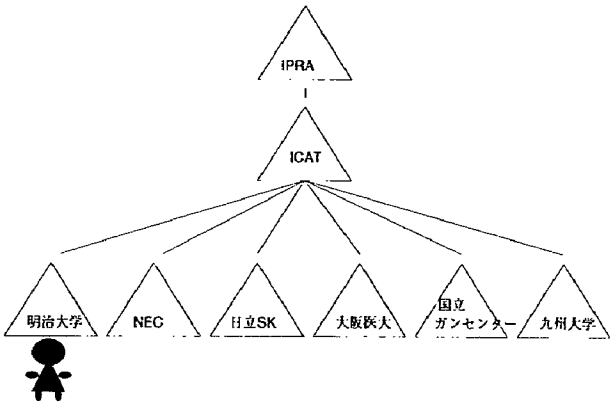
証明書の発行を複数の CA で分散して行う場合、CA 間の問い合わせ／返答のプロトコルをあらかじめ規定しておく必要がある。そこで我々は、HTTP（Hyper Text Transfer Protocol）をベースにした CA 間連携プロトコルを考察し、IETF へ提案した。

詳細については、文献[4]をご覧いただきたい。

2.4 実証実験

2.2で考察した 2 つのモデルを、検索速度、ネットワークトラフィック、スケーラビリティなどの点から比較・検討する為に、実証実験を行った。

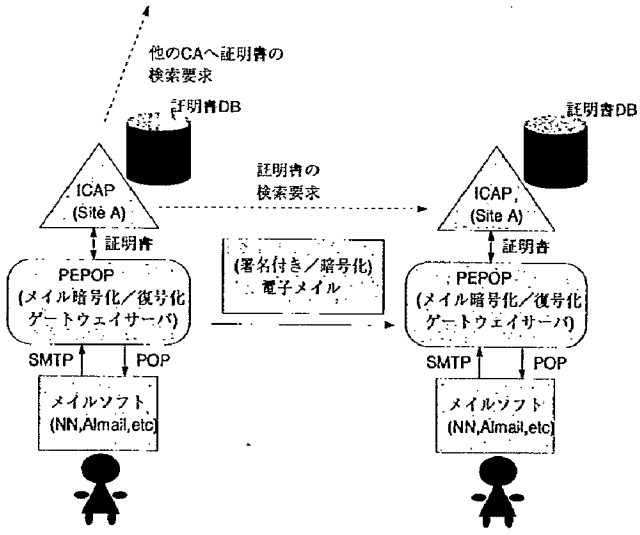
実証実験は、1998年 2 月 7 日、ICAT と医療情報通信研究会（JAMI）との共同で行った。実験に参加した組織、および CA 階層構造は、以下の図の通りである。



CA 構成図

実証実験は、ICAT で開発した PEPOP[3]という汎用暗号メイルゲートウェイプログラムを使用し、PEPOR から CA に証明書の検索要求があった時の、証明書の検索速度および上位 CA の CPU 負荷の値を計測することによって行った。

以下に実験の概要図を示す。



●実験概要図

実験の結果、以下の点が明らかになった。

1．モデル 2 は、モデル 1 よりも約1.5倍程度、上位 CA の CPU 負荷が大きくなった。これは下位 CA

の数が増えてくる程、モデル1の方が有利になると予想される。

2．検索速度については、モデル1とモデル2でさほど大きな差はでなかった。これは、検索速度におよぼす、上位CAのCPU負荷の違いによる影響よりも、上位CAと下位CA間のネットワーク遅延による影響の方が大きいためであると思われる。

3．ネットワークトラフィックに関しては、理論上、モデル1の方がモデル2よりも大きくなるが、証明書データのサイズは、1千数百バイトのオーダーである為、検索速度への影響は少なかった。

3．証明書を活用した認証サービスの実験

証明書を活用した認証サービスとして、メンバー限定のWebページに対するアクセスコントロールへの応用を試み、実験を行った。

詳細については、文献[5],[6],[7]をご覧いただきたい。

4．今後の予定

我々は、証明書発行局パッケージICAPにさまざまな改良を加えることによって、実証実験をおこなってきた。今後は、以下の点について考察を加えていくつもりである。

- CAにおける、安全な秘密鍵保持方法の検討。
- 他のディレクトリサービス（LDAPなど）との連携
- 証明書DBの強化

参考文献

(1) 服部裕之、櫻井三子、小林良至、菊池浩明：“オンライン証明書発行局パッケージ（ICAP）の実装と評価”、1997年暗号と情報セキュリティ・シンポジウム、SCIS'97-8C, (1997)

(2) 櫻井三子、服部裕之、小林良至、菊池浩明：“証明書発行局間の証明書情報共有機構の設計”、1997年暗号と情報セキュリティ・シンポジウム、SCIS'97-8D, (1997)

(3) 山崎直洋、菊池浩明、中西祥八朗：“暗号化サーバによる電子メールのプライバシ強化の提案”、1997年暗号と情報セキュリティ・シンポジウム、SCIS'97-8A, (1997)

(4) H. Kikuchi, M. Sakurai, Y. Sameshima, H. Hattori：*"Internet Public Key Infrastructure：Web-based Certificate and CRL Repository"*, Internet Draft, (1997) (available from ftp://ds.internic.net/internet-drafts/draft-kikuchi-web-cert-repository-00.txt)

(5) 服部裕之：“SSLeayとApacheによるセキュアサーバの構築について”、認証実用化実験協議会（ICAT）、'97定例研究会、(1997) (available from http://www.isc.meiji.ac.jp/~hhat/ppt/teirei_971)

(6) 櫻井三子、服部裕之：“moCA実験報告”、WIDE November'97研究会、(1997)

(7) 櫻井三子、服部裕之：“WIDEプロジェクトにおけるCA運用実験と考察”、1998年暗号と情報セキュリティ・シンポジウム、SCIS'98-3.3B, (1998)

(8) 明治大学実験CA：http://www.isc.meiji.ac.jp/ca/index.html